IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for analyzing a threat to system security, comprising:

identifying a threat agent having an existing access level attained by the threat agent in the course of an attack;

using the existing access level to analyze an attack path between the threat agent and an asset, including by:

setting an updated access level initially to the existing access level; and

iteratively comparing the updated access level with a required access level associated with a next attack along the attack path to determine whether the next attack along the attack path would be successful and, if so, updating the updated access level to equal a resulting access level associated with the next attack, until it is determined that the asset has been reached via the attack path or that no further attack along the path would be successful; and

in the event it is determined that the asset would be reached by the threat agent via the attack path, taking a responsive action in real time, prior to the asset actually being reached by the threat agent, the responsive action comprising a control or other countermeasure that results in the threat agent being rendered unable to reach the asset via the attack path;

wherein comparing the updated access level with a required access level associated with a next attack along the attack path includes determining the required access level associated with the next attack along the attack path at least in part by checking a stored controls data to determine whether an existing control applicable to the next attack along the attack path is in place and, if so, updating an initial, uncontrolled required access level associated with the next attack along the path to an updated required access level that reflects the effect of the control, wherein said step of updating is performed prior to the updated required access level being compared to the existing access level.

2. (Original) A method as recited in claim 1 wherein using the existing access level to analyze an attack path between the threat agent and an asset comprises identifying a vulnerability associated with the asset.

3. (Original) A method as recited in claim 1 wherein using the existing access level to analyze an attack path between the threat agent and an asset comprises identifying an exploit method associated with a vulnerability associated with the asset.

4. (Original) A method as recited in claim 3 wherein the exploit method has associated with it a prerequisite access level required to use the exploit method to exploit the vulnerability successfully.

5. (Original) A method as recited in claim 4 wherein using the existing access level to analyze an attack path between the threat agent and an asset comprises comparing the existing access level to the prerequisite access level.

6. (Canceled)

7. (Original) A method as recited in claim 3 wherein the exploit has associated with it a resulting access level that may be attained by using the exploit to exploit the vulnerability successfully.

8. (Original) A method as recited in claim 7 further including determining whether a control affects the resulting access level.

9. (Canceled)

10. (Canceled)

11. (Canceled)

12. (Original) A method as recited in claim 1 further including determining whether the asset is subject to compromise by the threat agent.

13. (Original) A method as recited in claim 1 further including determining whether a control affects the existing access level of the threat agent.

14. (Original) A method as recited in claim 13 further including updating the existing access level to reflect the affect of the control prior to using the existing access level to analyze an attack path between the threat agent and an asset.

15. (Original) A method as recited in claim 1 wherein identifying a threat agent comprises receiving from a network security system or application data comprising an identification of the threat agent.

16. (Original) A method as recited in claim 1 wherein identifying a threat agent comprises receiving from a network security system or application data that may be used to identify the threat agent.

17. (Original) A method as recited in claim 1 further including providing output data reflecting a result of the analysis of the attack path.

18. (Previously Presented) A method as recited in claim 17 wherein the output data comprises a report of the highest level of access that has been or could be achieved by the threat agent through one or more attacks along the attack path.

19. (Original) A method as recited in claim 1 wherein using the existing access level further includes evaluating recorded data to determine the attack path.

20. (Original) A method as recited in claim 1 wherein the attack path is determined by computing a transitive closure.

21. (Currently Amended) A computer program product for analyzing a threat to system security, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

identifying a threat agent having an existing access level attained by the threat agent in the course of an attack;

using the existing access level to analyze an attack path between the threat agent and an asset, including by:

setting an updated access level initially to the existing access level; and

iteratively comparing the updated access level with a required access level associated with a next attack along the attack path to determine whether the next attack along the attack path would be successful and, if so, updating the updated access level to equal a resulting access level associated with the next attack, until it is determined that the asset has been reached via the attack path or that no further attack along the path would be successful; and

in the event it is determined that the asset would be reached by the threat agent via the attack path, taking a responsive action in real time, prior to the asset actually being reached by the threat agent, the responsive action comprising a control or other countermeasure that results in the threat agent being rendered unable to reach the asset via the attack path;

wherein comparing the updated access level with a required access level associated with a next attack along the attack path includes determining the required access level associated with the next attack along the attack path at least in part by checking a stored controls data to determine whether an existing control applicable to the next attack along the attack path is in place and, if so, updating an initial, uncontrolled required access level associated with the next attack along the path to an updated required access level that reflects the effect of the control, wherein said step of updating is performed prior to the updated required access level being compared to the existing access level.